UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,120	12/17/2001	Tomoyuki Asano	SONY JP -139	6143

530 7590 08/28/2006

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,120	ASANO ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-9,12-16,19,22-26,29-33,36,39-43 and 46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-9,12-16,19,22-26,29-33,36,39-43 and 46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 178. Claims 47 – 101 and 137 – 138 have been withdrawn; claims 2, 3, 10, 11, 17, 18, 20, 21, 27, 28, 34, 35, 37, 38, 44, 45 and 102 – 136 have been canceled; and presently, pending claims are 1, 4 – 9, 12 – 16, 19, 22 – 26, 29 – 33, 36, 39 – 43 and 46.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/24/2006 has been entered.

Response to Argument

3. As per claims 1, 19, 36 and 46, Applicant alleged that Ginter does not teach the claim limitations as recited in the claim. Examiner notes Applicant's arguments have been fully considered but are not persuasive because the following crucial reasons, which are also presented during the phone interview with attorney Andrew T. Zidel on August 8, 2006:

- Ginter teaches "generates first integrity check values as integrity check values for a message including a usage policy obtained by a header of said content data and collates said first integrity check values to verify said message" (Ginter: Figure 26A / Element 948, Column 217 Line 51 – 52 and Column 137 Line 65 – 67: Method 1000 is the usage policy).
- Ginter teaches "generates second integrity check values as integrity check values for information including at least a content key obtained by a header of said content data and collates said second integrity check values to verify said information" (Ginter: Figure 26A / Element 950 – 980, Column 130 Line 39 – 40 and Column 152 Line 49 – 50 & Column 153 Line 8: the content keys are included in the PERC, which also contains the validation check value).
- Ginter teaches "generates an intermediate integrity check value based on said first integrity check values and said second integrity check values" (Ginter: Figure 26A / Element 980, Column 153 Line 9 – 10: PERC contains not only the access rights but also the content keys (as stated above), that can be validated by overall check value field 980 and as such the overall check value, as taught by Ginter, is equivalent to the intermediate integrity check value , as recited in the claim to meet the claim language).
- Therefore, in summary, "a first integrity check values, a second integrity check values and an intermediate integrity check value based on said first integrity check values and said second integrity check values" as recited in the claim are

indeed covered by Ginter's reference as shown on Figure 26A and Figure 26B and as such Applicant's arguments are respectfully traversed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 4, 7, 12, 16, 19, 22, 24, 29, 33, 36, 39, 41 and 46 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter et al. (U.S. Patent 6,253,193).

As per claim 1, 19, 36 and 46, Ginter teaches a data processing apparatus for processing content data provided by a recording or communication medium, characterized in that said apparatus comprises:

a cryptography process section for executing a cryptography process on said content data (Ginter: Column 15 Line 37 – 38); and

a control section for executing control for said cryptography process section (Ginter: Column 5 Line 24 – 27 and Column 6 Line 17 – 31), and

said cryptography process section:

generates first integrity check values as integrity check values for a message including a usage policy obtained by a header of said content data (Ginter: Figure 17, Column 149 Line 1 – 7, Figure 26A Element 978 and Column 217 Line 51 – 52 / Line 59 – 60),

collates said first integrity check values to verify said message (Ginter: Column 217 Line 51 – 52 / Line 59 – 60),

generates second integrity check values as integrity check values for information including at least a content key obtained by a header of said content data (Ginter: Figure 17, Column 149 Line 1 – 7, Figure 26A / Element 906a/b, Figure 26B Element 912 / Element 994: Note: Figure 26B, which includes content key, is an example of one of right records),

collates said second integrity check values to verify said information (Ginter: Column 217 Line 51 – 52 / Line 59 – 60),

generates an intermediate integrity check value based on said first integrity check values and said second integrity check values (Ginter: Figure 26A / Element 980, and Column 153 Line 9 – 13), and

uses the generated intermediate integrity check value to verify said content data corresponding to said first and second integrity check values (Ginter: Column 153 Line 9 – 13 and Column 217 Line 51 – 52 / Line 59 – 60).

As per claim 4, 22 and 39, Ginter teaches said cryptography process is a DES cryptography process, and said cryptography process section is configured to execute the DES cryptography process (Ginter: Column 22 Line 8 – 13).

As per claim 7, 24 and 41, Ginter teaches said data processing apparatus has a signature key, and said cryptography process section: is configured to apply a value generated from said intermediate value by means of said signature key-applied cryptography process as a collation value for data verification (Ginter: Column 22 Line 12 – 25).

As per claim 12 and 29, Ginter teaches a recording device for storing data validated by said cryptography process section (Ginter: Column 28 Line 38 – 41).

As per claim 16 and 33, Ginter teaches collating only the header section integrity check values in the data during the process executed by said cryptography process section to collate said first integrity check values and said second integrity check values (Ginter: Figure 17, Column 149 Line 1 – 7, Figure 26A Element 978 and Column 217 Line 51 – 52 / Line 59 – 60 and Figure 26B Element 912 / Element 994: Note: Figure 26B, which includes content key, is an example of one of right records).

transmitting data for which collation of the header section integrity check values has been established, to said reproduction process section for reproduction (Ginter: Column 28 Line 38 – 41 and Ginter: Figure 17, Column 149 Line 1 – 7, Figure 26A

Element 978 and Column 217 Line 51 – 52 / Line 59 – 60: the data is decrypted (and copied to CD-ROM subsequently) only after the header section check value (or validation tag) is not tempered)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5, 6, 23 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al. (U.S. Patent 6,253,193), in view of Teppler (U.S. Patent 6,898,709).

As per claim 5, 23 and 40, Ginter does not disclose expressly said partial integrity check value is a message authentication code (MAC) generated in an DES-CBC mode using partial data to be checked, as a message, said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message, and said cryptography process section is configured to execute the cryptography process in the DES-CBS mode.

Teppler teaches said partial integrity check value is a message authentication code (MAC) generated in an DES-CBC mode using partial data to be checked, as a message, said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message, and said cryptography process section is configured to execute the cryptography process in the DES-CBS mode (Teppler: Column 30 Line 48 – 53).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Teppler within the system of Ginter because Teppler teaches providing the assurance of the integrity of digital data files with enhanced fraud prevention mechanisms (Teppler: Column 16 Line 36 – 52).

As per claim 6, Ginter as modified teaches in the DES-CBC mode-based cryptography process configuration of said cryptography process section, Triple DES is applied only in part of a message string to be processed (Teppler: Column 30 Line 48 – 53 and (Teppler: Column 7 Line 12 – 24).

6. Claims 8, 25 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al. (U.S. Patent 6,253,193), in view of Orrin (U.S. Patent 6,011,849).

As per claim 8, 25 and 42, Ginter does not disclose expressly said data processing apparatus has a plurality of different signature keys as signature keys, and said cryptography process section: is configured to apply one of said plurality of

different signature keys which is selected depending on a localization of said content data, to the cryptography process for said intermediate integrity check value to obtain the collation value for data verification.

Orrin teaches said data processing apparatus has a plurality of different signature keys as signature keys, and said cryptography process section: is configured to apply one of said plurality of different signature keys which is selected depending on a localization of said content data, to the cryptography process for said intermediate integrity check value to obtain the collation value for data verification (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Orrin within the system of Ginter because Orrin teaches providing an easy-to-use interface and easy-to-integrate environment for file and document encryption including partial content encryption during communications and the assurance of the integrity of digital data files with enhanced fraud prevention mechanisms (Orrin: Column 3 Line 4 – 11 and Column 16 Line 36 – 52).

7. Claims 9, 26 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al. (U.S. Patent 6,253,193), in view of Orrin (U.S. Patent 6,011,849), and in view of Kuroda (Patent Number: 6915434).

As per claim 9, 26 and 43, Ginter as modified does not disclose expressly said data processing apparatus has a common signature key common to all entities of a

system for executing a data verifying process and an apparatus-specific signature key specific to each apparatus that executes a data verifying process.

Kuroda teaches said data processing apparatus has a common signature key common to all entities of a system for executing a data verifying process and an apparatus-specific signature key specific to each apparatus that executes a data verifying process (Kuroda: Abstract Line 1 – 10);

said selecting step being based on the location of said content data (Orrin: Abstract Line 7 – 8, Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kuroda within the system of Ginter as modified because Kuroda teaches providing a key management function in an electronic data storage system for guaranteeing the security of electronic data by changing the key used in a process of encrypting electronic data in document form in a local environment and a global environment (Kuroda: Column 1 Line 10 – 16).

8. Claims 13 – 15 and 30 – 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al. (U.S. Patent 6,253,193), in view of Bodo (Patent Number: 5680587).

As per claim 13 and 30, Ginter does not disclose expressly said control section suspends storing of aid data in said recording device if a process of collating said first

integrity check values and said second integrity check values is not established in said cryptography process executed by said cryptography process section.

Bodo teaches said control section suspends storing of said data in said recording device if a process of collating said first integrity check values and said second integrity check values is not established in said cryptography process executed by said cryptography process section (Bodo: Column 13 Line 16 – 25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bodo within the system of Ginter because (a) Ginter discloses invoking secure digital data content backup to removable media such as CD-ROM (Ginter: Column 28 Line 38 – 41) and (b) Bodo teaches an enhanced-performance removable media subsystem for securely recording the digital data (Bodo: Column 13 Line 16 – 25).

As per claim 14 and 31, claims 14 and 31 do not further teach over claims 13 as addressed above

As per claim 15 and 32, claims 15 and 32 do not further teach over claims 13 as addressed above

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100